Common Result Format (CRF) Discussion

September, 2008

David Waltermire

A standard is needed to encode standardized asset reporting data

- Provide a consistent data interchange format for asset data
- Support creation of standardized reporting interfaces to allow interoperability between tools
- Enable enterprise and regulatory reporting

Reporting Requirements

- Report findings from automated vulnerability scans
- Report findings from compliance assessments

- Replace existing US Government specific reporting formats with a single generalized format:
  - FDCC Reporting
  - DoD VMS XML reporting format

Data Model Requirements

The data model MUST:

- Be based on a standard asset model
- Support summarizing/repackaging XCCDF and check results
- Minimize data duplication through use of references
- Support multiple, possibly pre-defined, levels of abstraction
- Support reporting at different levels of granularity
- Support network and organizational-related vulnerabilities and configuration controls
- Indicate the result of mitigations, POA&Ms/risk acceptance, and references to persistent exceptions
- Support source authentication & data integrity
- Specifies whether reported results are outcomes of assessments or other assertions

The data model must be based on a standard asset model

- Must support standardized outputs across multiple vendor tools and types of tools

Possible models include:

- DoD Asset Model 0.3
- Asset Reporting Format (ARF)
- Others?

The data model must support summarizing/repackaging XCCDF and check results

- Provide pass/fail status for XCCDF rules
  - CCI, CCE, and CVE IDs
  - SP 800-53 controls
- Support references to detailed XCCDF and check system results
- Allow drill down to XCCDF and OVAL artifacts

The data model must minimize data duplication through use of references

- Each document/object reported only once
- Object types:
  - Assets
  - Facility
  - Geo-location
  - Network
  - Organization
  - Person
  - POA&M
  - Policy
  - Others?

The data model must support multiple levels of abstraction

- Network
- Organizational Unit
- System
- Enterprise wide
- Others?

- Predefined or ad hoc levels?

The data model must support reporting at different levels of granularity

- Counts
- Individual devices
- Groupings
- Others?

The data model must support network and organizational-related vulnerabilities and configuration controls

- Individual devices
- Network architectural issues
- Operational and management controls

The data model must indicate the result of mitigations, POA&Ms/risk acceptance, and references to persistent exceptions

- Must be capable of referencing an old finding
- Must indicate the POA&M generated for a finding

The data model must support source authentication and data integrity

- Must indicate the tool that generated results
- Must reference the content and content version that was assessed
- Must reference the results and time of the assessment
- XML Signatures?
- Tool certificates?

The data model must specify whether reported results are outcomes of assessments or other assertions

- Need to establish attribution for result
  - Results generated automatically
  - Results generated using an interrogative check schema
  - Results were automatically generated but manually interpreted

Machine Interface Requirements

Machine interfaces MUST:

- Support standardized communications between disparate tool types
- Support transmission and drill-down capabilities to lower levels of detail
- Ability to operate in constrained environments
- Support authentication, confidentiality & non-repudiation (trusted path establishment vs trusting data objects)

Machine interfaces must provide support for standardized communications between disparate tool types

- Publication
- Query at multiple levels of abstraction
- Other interfaces?

- Vulnerability scanners
- Compliance assessment tools
- SCAP result databases
- Human-readable report generators

Machine interfaces must support transmission of and drill-down to lower levels of detail

Must support transmission and retrieval of:

- XCCDF results
- Check system results
- Remediation results
- Others?

Machine interfaces must have the ability to operate in constrained environments

- High security environments
- Restricted network connectivity
- Push vs. Pull
- Low bandwidth
    - Transmission of result deltas since the last assessment report
    - Compression
- Support paging for human interfaces

Machine interfaces must support authentication, confidentiality, and non-repudiation

- Trusted path establishment vs signing data objects
- Encryption of data stream and content at rest
- Certificate authentication and revocation

Important CRF Information

Current Specification: http://crf.mitre.org

SCAP Discussion List:

http://nvd.nist.gov/home.cfm?emaillist

Presenter:

David Waltermire

david.waltermire@nist.gov